UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
CRIMINAL NO 21-133 (DWF/DTS)

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff	)	
	)	
v.	)	**DEFENDANT'S MEMORANDUM**
	)	**IN SUPPORT OF OBJECTIONS**
NATHAN DOBBELMANN	)	**TO REPORT AND**
	)	**RECOMMENDATION**
Defendant	)	

INTRODUCTION AND SUMMARY OF ARGUMENT

On July 6, 2021, Defendant Nathan Miller Dobbelmann filed motions to suppress evidence discovered during the search of two Snapchat user accounts and a Black Samsung cell phone. *ECF No. 30*. During the August 3, 2021, motions hearing, the motions to suppress were tendered to the Magistrate Judge on the four corners of the respective search warrants and no evidentiary hearing was held. On September 17, 2021, Magistrate Judge Schultz issued a Report & Recommendation ("R&R") recommending that Mr. Dobbelmann's motions be denied. *ECF No. 38*.

The following memorandum provides the legal basis for Mr. Dobbelmann's objections to the Report and Recommendation. As set forth below, the affidavit supporting the search warrants for the Snapchat user accounts ("Affidavit") failed to establish probable cause because: (1) the Affidavit did not demonstrate a fair probability that evidence of a crime would be found in either

Snapchat account; and (2) the Affidavit did not show the requisite nexus between the contraband (child pornography) and the Snapchat accounts. This lack of probable cause was so apparent that a reasonable officer could not have objectively relied upon the issuing judge's probable cause determination. As a result, the good faith exception does not prevent the suppression of evidence obtained from the searches of the Snapchat accounts.

Similarly, the search warrant to search the Black Samsung cell phone also lacked probable cause because that warrant relied on information from a third party that was too vague, uncertain and unreliable to establish probable cause.

BACKGROUND FACTS

On November 4, 2020, Special Agent Matthew Vogel filed an affidavit in support of an application for a search warrant seeking information from two Snapchat user accounts that the Government's investigation had linked to Mr. Dobbelmann. *See Government's Exhibit 2, ECF No. 33-2*. This investigation began on August 28, 2020, when an undercover officer ("UC") accessed a chat room on a "foreign-housed chat application.[1] *Id, ¶12*. During the next two days, the UC observed third parties post links to folders contained large amounts of child pornography files. *Id., ¶13-14.* One of the 165 participants in the chat room was a participant who used the screen name ILIVERICHOUSLY. *Id. at ¶15*. For an unstated reason, the UC initiated contact with ILIVERICHOUSLY by sending a direct message stating his interest in child pornography and asking

[1] The Affidavit did not name the foreign-housed application due to the concerns

ILIVERICHOUSLY to contact him on the KIK messaging application. *Id. at 16*. ILIVERICHOUSLY responded to the UC's direct message (on the foreign-housed app) on September 6, 2020. *Id. at 17*. ILIVERICHOUSLY's first message stated it was nice to hear from you and then asked the UC about his children and if the UC had pictures of the children. *Id. at p. 10*. In subsequent messages, ILIVERICHOUSLY told the UC his age, that he lived in Minnesota, that he was interested in joining the UC and his wife and daughter, and that he wanted pictures of the UC's daughter in exchange for pictures that he would send to the UC. *Id*. To persuade the UC to send him these photos, ILIVERICHOUSLY messaged that he was going to send the UC several pictures of himself in order to gain the UC's trust:

> *Here are a few pix of me. Here are a bunch if me for you so i hope you trust a bit more.*

Id., ¶17 at p. 11. ILIVERICHOUSLY then sent the UC multiple images, including images of himself engaged in sex with adult females. *Id*. "Several" of these images contained a QR code. *Id*. When the UC sent a message complaining these images were adult porn and that he wanted "OC" (original content), ILIVERICHOUSLY sent the UC three videos containing graphic child pornography. *Id., at p. 13*. Neither ILIVERICHOUSLY nor the UC remarked on QR code or mentioned the Snapchat application. *See Id*. Instead, the UC continued his attempt to direct ILIVERICHOUSLY to the KIK application:

"u have KIK;"
* * *
"u have KIK, mine is XXXXXXX"
* * *

"U got KIK"
* * *
"U got KIK, Mine is XXXXXXX"

See Id. at ¶17, pp. 10-11 and 13. After the UC's fourth attempt to direct ILIVERICHOUSLY to KIK, the UC gave his KIK username and asked ILIVERICHOUSLY for his. *Id at p. 13*. ILIVERICHOUSLY responded by messaging the UC that his KIK username was "extremepussypleaser." *Id*.

On or about September 23, 2020, the UC received a message on his KIK account stating "He this is iliverichously on [foreign chat service] whatcha got to share with me." *Id., ¶19 at p. 14*. In the ensuing chat conversation, the UC asked "extremepussypleaser" if he was a parent, to which extremepussypleaser responded by giving details about his family and asking the UC for "sexy pictures and videos of your daughter??" *Id*. Neither ILIVERICHOUSLY nor the UC mention the Snapchat application during their conversation on KIK. *See Id*.

At an unspecified time after iliverichously contacted the UC on KIK, the UC "captured" extremepussypleaser's KIK profile information, which included the name "NoExpectationsNoLimitationssnap@awesomedaddy198." Id. ¶20. On another unspecified date, the FBI served an administrative subpoena on the operator of the KIK messenger application for information on extremepussypleaser's KIK account and received the following information:

First Name: NoExpectationsNoLimitations
Last Name: snap@awesomedaddy198[10]
Email: awesomedaddy1981@yahoo.com (confirmed)

Id. at ¶25, pp. 16-17. Referring to the Snapchat user name listed in the "Last Name" field, SA Vogel stated: "[f]rom my training and experience, I am aware that this is a directive for others to contact the user on Snapchat account awesomedaddy198." *Id. at p. 17, note 10*.

On October 28, 2020, SA Vogel scanned the QR code present in several of the images that ILIVERICHOUSLY had sent to the UC on September 6. *See Id.*, *¶17, 18*. At that time, SA Vogel learned the QR code directed to the publicly available Snapchat account with the username Iliverichously. *Id*.

ARGUMENT

I. THE R&R ERRED WHEN IT RECOMMENDED THAT THIS COURT DENY MR. DOBBELMANN'S MOTION TO SUPPRESS EVIDENCE DISCOVERED DURING THE SEARCH OF TWO SNAPCHAT USER ACCOUNTS.

A. Standard of Review.

A valid search warrant must be supported by probable cause, which exists "if under the totality of the circumstances, a showing of facts can be made `sufficient to create a fair probability that evidence of a crime will be found in the place to be searched." *United States v. Wallace,* 550 F.3d 729, 732 (8th Cir. 2008) (quoting *United States v. Underwood,* 364 F.3d 956, 963 (8th Cir. 2004). An issuing court's probable cause determination should be paid great deference. *United States v. Johnson*, 848 F.3d 872, 876 (8th Cir. 2017.) "Deference to the magistrate, however, is not boundless." *United States v. Leon*, 468 U.S. 897, 914. "[R]eviewing courts will not defer to a warrant based on an affidavit that does not provide the magistrate with a substantial basis for determining the existence of probable

cause." *Id. at 915* (internal quotation marks omitted.)

B. The Affidavit Supporting the Warrant Application Failed To Show A Fair Probability That Evidence Of A Crime Would Be Found In The Two Snapchat Accounts.

Though establishing probable cause "is not a high bar," (*Kaley v. United States, 571 U.S. 320, 338 (2014*)), it still requires "a showing of facts" that "create a fair probability that evidence of a crime will be found in the place to be searched." *United States v. Wallace*, 550 F.3d 729, 732 (8th Cir. 2008). The Affidavit supporting the Snapchat warrants fails to meet this requirement.

Before proceeding with the analysis, it is necessary to clarify what "evidence of a crime" refers to in the context of the Snapchat search warrant at issue. The Affidavit makes no claim that police were aware any of child pornography related activity taking place on either Snapchat account. This necessarily means that police would have no way of knowing whether the other information sought by the warrant (subscriber information, IP addresses, activity logs, IP logs, location data, etc.…) might be evidence of a specific crime. As a result, "evidence of a crime" for purposes of analyzing the Snapchat warrants is limited to child pornography and communications expressly referencing child pornography.

Returning to the analysis, the R&R found it was reasonable to infer that child pornography would be found on Snapchat accounts because police had linked ILIVERICHOUSLY to these accounts and the online participant had shared the account information with the UC:

> *The warrant for the Snapchat account is based on the fact that the online participant sharing and requesting images and videos of child pornography was linked to two Snapchat accounts with profile pictures that appear to include Dobbelmann. The online participant shared the Snapchat account information with the UC while in an online chat room where child pornography was being traded. It was reasonable for the issuing judge to infer that it was fairly probable that child pornography would be found by accessing the Snapchat account information.*

R&R at p. 4.[2]

The R&R's conclusion is flawed because it does not explain how linking the Snapchat accounts to the online participant, and the "sharing" of that information with the UC, allow an inference that child pornography would be found on those accounts. Indeed, examination of the totality of the circumstances shows that such an inference is not possible.

First, the Affidavit contains no information indicating police had knowledge of any criminal activity occurring on either Snapchat account. Second, neither ILIVERICHOUSLY/extremepussypleaser nor the UC mentioned Snapchat during any of their lengthy (and recorded) chats on two other messaging applications. *See Gov. Exhibit. 2, at ¶¶17, 19*. Third, while messaging candidly about identifying information and his other predilections, ILIVERICHOUSLY never mentioned he had Snapchat accounts and never attempted to direct the UC to these accounts, even after the UC sought, five times, to steer him to the KIK application.

The best, and only argument for finding probable cause is that

[2] As noted in Mr. Dobbelmann's Objections to the Report and Recommendation, The Magistrate Judge erred when he found that the two Snapchat accounts had profile pictures of Mr. Dobbelmann. Snapchat profiles use emojis, not photos.

ILIVERICHOUSLY/extremepussypleaser shared the Snapchat account information for the purpose of directing the UC to contact at him on these accounts for child pornography purposes. *See Government's Consolidated Response to Defendant's Pretrial Motions*, at p. 16, ECF No. 33. ("ILIVERICHOUSLY/extremepussypleaser directed others to these accounts himself in the very communications in which he sent or asked for child pornography.") Again, the circumstances outlined in the Affidavit, when viewed in their totality, do not support such a argument.

The Affidavit reveals the Snapchat account information came to light in three ways: (1) when the UC "captured" extremepussypleaser's KIK profile name; (2) on October 28, 2020, when Special Agent Vogel scanned the QR code embedded in some of the images ILIVERICHOUSLY had sent to the UC; and (3) on an unspecified date after the FBI served an administrative subpoena on the company that owns KIK. *See Government Exhibit 2, ¶¶18, 20 and 25*. Examination of the totality of the circumstances surrounding each transmission of Snapchat account information shows that it is not reasonable to infer that ILIVERICHOUSLY/extremepussypleaser intended to direct anyone to the target Snapchat accounts.

Turning first to the UC's capture of ILIVERICHOUSLY's KIK profile. The Affidavit makes no claim that use of another social media account information in a KIK profile name signifies an intent to direct others to that account. Moreover, the fact that the UC captured the username without ILIVERICHOUSLY's

knowledge obviates any inference that the latter sought to direct the UC to the Snapchat account.

Similarly, there is nothing in the circumstances surrounding the QR code contained in the photos ILIVERICHOUSLY sent the UC on September 6, 2020, that indicate an intent to direct the UC to a Snapchat account. *See Gov Exhibit 2, ¶17*. Neither ILIVERICHOUSLY nor the undercover officer mentioned the QR codes or the Snapchat application, and the UC did not think to scan the QR codes even though he was actively investigating the case. The fact that authorities did not scan the QR code until nearly two months later (see *Id., ¶18*), is no slight on the investigation, but instead highlights the fact that an experienced undercover officer did not view the QR codes as an invitation or direction.

Lastly, the FBI served an administrative subpoena and obtained subscriber information about extremepussypleaser's KIK account, including the following:

> First Name: NoExpectationsNoLimitations
> Last Name: snap@awesomedaddy198[10]
> Email: awesomedaddy1981@yahoo.com (confirmed)

Id., ¶25. In a footnote after the last name field, SA Vogel wrote "[f]rom my training and experience, I am aware that this is a directive for others to contact the user on Snapchat account awesomedaddy198." *Id. at p. 18 note 10*. It is significant that this is the only one of the three Snapchat account transmissions that SA Vogel believed signified a directive to others. Even more significant, SA Vogel's belief is wrong in this instance because the information he cites is not

available to other KIK users. KIK's Law Enforcement Guide indicates that KIK does not share personal information such as first names, last names or email addresses, to other users:

> *Unlike many other smartphone messaging services which are based on a user's phone number, Kik uses usernames as the unique identifier. By using usernames instead of phone numbers, users' personal information is never shared by Kik.*

KIK Law Enforcement Guide, at p. 2.[3] The unavailability of this information to KIK's users is also shown by the fact that the FBI needed to get an administrative subpoena to obtain this information.[4]

In conclusion, the only information that police had about the target Snapchat accounts was that ILIVERICHOUSLY/extremepussypleaser was linked to these accounts. This is not sufficient to establish probable cause to search these accounts. *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought.") As a result, the Snapchat search warrant is invalid.

---

[3] Available at https://www.kik.com/uploads/files/Kik-Law-Enforcement-Guide-Revised-Feb-2021.pdf (last accessed 10/1/21).

[4] Per the Affidavit, Snapchat has a similar privacy policy:

> Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users.

Gov. Exhibit 2, at p. 4-5.

C. The Supporting Affidavit Failed To Show A Nexus Between The Evidence Of Illegal Activity And The Target Snapchat Accounts.

There must be evidence of a nexus between the contraband and the place to be searched before a warrant may properly issue. *United States v. Summage*, 481 F.3d 1075, (8th Cir. 2017) citing *United States v. Tellez*, 217 F.3d 547 (8th Cir. 2000). The connection between the location to be searched and the contraband must be specific and concrete, not vague or generalized. *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016). Examination of the Affidavit shows that it also failed to satisfy this nexus requirement.

Factors to consider in determining if a nexus exists include "the nature of the crime and the reasonable, logical likelihood of finding useful evidence." United *States v. Johnson*, 848 F.3d 872, 878 (8th Cir. 2017) (quoting *United States v. Tellez,* 217 F.3d at 550). Both of these factors weigh against finding the requisite nexus.

With regard to the nature of the crime factor, one common characteristic of child pornography offenders is that they retain their child pornography collections for long periods of time. *See generally United States v. Chrobak*, 289 F.3d 1043, 1046 (8th Cir. 2002) ("Child pornographers generally retain their pornography for extended periods"); *United States v. Summage,* 481 F.3d 1078, 1078 (8th Cir. 2007) (presuming the defendant "would maintain in his possession the video and photographs that he made of the sexual encounter"). Of the many social media applications widely available, Snapchat is perhaps the most ill

suited for persons interested in child pornography because of its widely known feature of immediate deletion of messages:

> *Delete is our default . . .This means most messages sent over Snapchat will be automatically deleted once they've been viewed or have expired. Here are some quick rules of thumb for how long different kinds of content stays on Snapchat servers!*

Snapchat Support, "When does Snapchat delete Snaps and Chats," available at https://support.snapchat.com/en-US/article/when-are-snaps-chats-deleted (last accessed 10/1/21). The Affidavit verifies this Snapchat feature, outlining each of the four main types of messages available on Snapchat (Snaps, Stories, Memories and Chats), and then describing how each type of message (except for "Stories") are automatically deleted unless the user takes an affirmative step to save the message. *Gov. Exhibit 2, pp. 3-4*. While Snapchat does allow users to take steps to retain messages, many users, as the Affidavit acknowledges, do not know this:

> *Based on my training and experience, I know that many users of Snapchat initially believe that almost all communications, including images and videos they send through the Snapchat app are automatically deleted after a certain amount of time.*

Id. ¶8 at p. 5.

Given this defining characteristic of Snapchat, persons involved in child pornography offenses are unlikely to use Snapchat when there are many other applications better suited to facilitating their crimes. Accordingly, the second factor, the likelihood that police will find useful evidence, weighs against finding a nexus and further precludes a finding of probable cause.

II. THE GOOD FAITH EXCEPTION DOES NOT SAVE THE SEARCH WARRANT.

Under the good faith exception, evidence obtained under an invalid search warrant need not be suppressed when an officer acts "in objectively reasonable reliance on a subsequently invalidated search warrant . . ." *United States v. Leon*, 468 U.S. 897, 922 (1984). "The good-faith exception does not, however, create a blanket exemption against suppression whenever police officers search pursuant to a warrant." *United States v. Scroggins*, 361 F.3d 1075, 1083 (8th Cir. 2004) (citing *Leon*, 468 U.S. at 922); *See United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996) (The good faith exception "is not a magic lamp for police officers to rub whenever they find themselves in trouble.")

There are four circumstances in which the *Leon* good faith exception does not apply and suppression remains an appropriate remedy: (1) the magistrate judge issuing the warrant was misled by statements made by the affiant that were false or made "in reckless disregard for the truth"; (2) "the issuing magistrate judge wholly abandoned his [or her] judicial role"; (3) the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or (4) the warrant is "so facially deficient . . . that the executing officers cannot reasonably presume it to be valid." *United States v. Riedesel*, 987 F.2d 1383, 1391 (8th Cir. 1993) (quoting *Leon*, 468 U.S. at 923).

In recent years, Courts have been reluctant to apply the exclusionary rule in cases involving search warrants for social media. *See United States v. Chavez*, 423 F.Supp.3d 194, 208 (W.D. N.C. 2019) ("[A]pplying the Fourth Amendment to

social media accounts is a relatively unexplored area of law with nuances that have yet to be discovered."); *United States v. Westley*, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *17 (D. Conn. July 17, 2018) ("[T]he application of search warrants to Facebook accounts is a relatively new area of the law.") This Affidavit does not, however, present a situation where the clear lack of probable cause can be attributed to inexperience with new social media technology or an undiscovered nuance. Instead, the Affidavit is flawed because it fails to fulfill the basic and well-known requirements that it show why evidence might be discovered in a particular place and a nexus between the evidence sought and the place to be searched be established. Given these deficiencies, and the other circumstances discussed in these objections, any officer executing the Snapchat warrants could not have "reasonably rel[ied] upon the issuing court's determination of probable cause for a search warrant." *United States v. Herron*, 215 F.3d 812, 814-15 (8th Cir. 2000) (concluding that the good-faith exception did not apply because "the lack of probable cause in the affidavits would have been apparent to reasonable officers" where the affidavits lacked information about the defendant and his residence).

III. THE R&R ERRED WHEN IT RECOMMENDED THAT THIS COURT DENY MR. DOBBELMANN'S MOTION TO SUPPRESS EVIDENCE DISCOVERED DURING THE SEARCH OF BLACK SAMSUNG CELL PHONE.

Mr. Dobblemann also moved to suppress the search of a black Samsung cell phone that a third party gave to police. See Defendant's Motion to Suppress, p. 2, ECF No. 30. Mr. Dobbelmann's objections to the Magistrate Judge's

recommendation that this motion be denied hereby incorporates and references the arguments made in his initial motion to suppress.

CONCLUSION

Based upon the preceding objections, Mr. Dobbelmann respectfully objects to the Magistrate Judge's recommendation that this Court deny his motions to suppress.

Dated: October 1, 2021.

JOHNSON & GREENBERG, PLLP

s/Lee R. Johnson_____
Lee R. Johnson #189935
5775 Wayzata Boulevard
Suite 700
St. Louis Park, MN 55416
(952) 545-1621

Attorney for Defendant
Nathan Miller Dobbelmann